

STEGANALISIS PADA CITRA DIGITAL DENGAN FORMAT JPEG MENGUNAKAN UJI CHI-SQUARE

Nailah Arifah¹, Bambang Hidayat², Suci Aulia³

¹Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Steganalisis merupakan ilmu yang dilakukan untuk mengidentifikasi ada atau tidaknya pesan tersembunyi dalam suatu data (file). Ada banyak metode yang dapat dilakukan dalam steganalisis pada berbagai macam domain. Sedangkan, teknik steganografi yang sering digunakan adalah steganografi dengan menggunakan metode Least Significant Bit dalam domain spasial maupun DCT yang dinamakan metode Jsteg.

Oleh karena itu, dalam tugas akhir ini saya akan menganalisis keakuratan metode dari steganalisis pada citra digital yang disisipi pesan rahasia menggunakan metode JSteg dan menganalisis dengan metode Chi-square Tests. Analisis akan dilakukan pada file-file image dengan format image JPEG atau JPG.

Model terbaik pada metode ini adalah pada saat menggunakan skema 2 dengan nilai $\alpha=0.88$, yaitu akurasi persentase mencapai 88,65716%. Namun penggunaan skema 1 lebih baik, karena kestabilan pada nilai p-valuenya. Akurasi tertinggi menggunakan skema 1 adalah saat menggunakan $\alpha=0.75$ yaitu 85,37449%. Akurasi deteksi tertinggi yaitu pada saat menggunakan skema 1, yaitu mencapai 100% pada citra non stego dengan background non statis dan 33,33% untuk background statis serta 100% pada citra stego untuk keduanya. Namun, waktu yang dibutuhkan untuk pengujian menggunakan skema 1 lebih lama dari skema 2.

Kata Kunci : steganalisis, JSteg, Uji Chi-square

Abstract

Steganalysis is a science that is carried out to identify whether there is any hidden messages in the data (files). There are many methods that can be done in steganalysis on various domains. Meanwhile, steganography technique that is often used is steganography by using the Least Significant Bit in the spatial domain or the DCT called Jsteg method.

Therefore, in this thesis I will analyze the accuracy of the steganalysis methods in digital image inserted a secret message using JSteg methods and analyzing the method of Chi-square Tests.

The analysis will be performed on image files to JPEG or JPG image format.

The best model is the method when using second scheme with a value of $\alpha=0.88$, which reached 88,65716% accuracy. However, the use of first scheme is better, because the stability of that p-value. The highest accuracy using first scheme is when using $\alpha = 0.75$ and reached 85,37449% accuracy. The highest detection accuracy when using scheme 1, reaching 100% in non-stego images with non-static backgrounds and 33.33% for the static background as well as 100% for both the stego image. However, the time required to test using scheme 1 longer than scheme 2.

Keywords : steganalysis, JSteg, Chi-square Test

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Saat ini pertukaran data dapat dilakukan dengan sangat mudah. Misalnya saja, saat ini sudah banyak cara untuk mengirimkan suatu data dari pengirim ke penerima yang ada pada jarak cukup jauh. Salah satunya adalah melalui internet. Data berupa teks, citra, audio, maupun video pun dapat dikirimkan kepada seseorang yang berada pada jarak yang jauh dari pengirim namun dalam bentuk digital. Sebuah data digital yang bersifat rahasia pun saat ini dapat dikirimkan dengan berbagai cara, salah satunya adalah steganografi.

Steganografi dapat mengirimkan data dengan menggunakan teknik penyembunyian pesan yang berupa teks, citra, audio ataupun video ke dalam sebuah media lain yang dapat berupa teks, citra, audio maupun video juga. Teknik steganografi berkembang sangatlah cepat. Bahkan sudah banyak aplikasi gratis yang mudah sekali di unduh melalui internet untuk melakukan steganografi. Aplikasi tersebut dapat digunakan dengan mudah dan tidak terlalu mengurangi ketahanan dari pesan rahasia. Namun kemudahan itu terkadang dimanfaatkan untuk melakukan tindak kriminal contohnya digunakan untuk komunikasi perdagangan narkoba dan penyisipan gambar porno.

Oleh karena permasalahan di atas, diperlukan pendeteksian *file-file* yang mencurigakan untuk dipastikan bahwa tidak ada data rahasia yang dikirimkan yang dibungkus oleh media lain. Steganalisis merupakan ilmu atau seni yang dapat mengatasi permasalahan ini. Steganalisis dapat mengetahui, apakah dalam satu *file* terdapat pesan rahasia atau tidak.

Pada umumnya objek pembungkus pesan rahasia adalah citra dengan metode steganografi yang digunakan adalah metode *Least Significant Bit* pada domain *spatial* dan *Jsteg* pada domain DCT. Metode *Jsteg* merupakan pengembangan dari metode LSB dan dapat digunakan pada citra dengan format jpg. Oleh karena itu, pada tugas akhir ini akan dilakukan steganalisis pada beberapa *file* citra menggunakan metode *Uji Chi-square analysis* dengan menguji *file* stego menggunakan metode *Jsteg*.

1.2 Rumusan Masalah

Pada steganalisis ini, dibutuhkan beberapa sampel citra digital yang tidak disisipi oleh pesan rahasia dan citra digital yang sudah disisipi pesan rahasia. Oleh karena itu, pada tugas akhir ini akan dianalisis mengenai:

1. bagaimana steganalisis menggunakan metode Uji *Chi-square* pada citra .jpg?
2. bagaimana hasil persentase analisis suatu citra menggunakan Uji *Chi-square* dengan menggunakan domain DCT (frekuensi) dengan persentase sisipan yang berbeda-beda?
3. bagaimana karakteristik citra yang berpotensi terdeteksi dengan benar dan bagaimana karakteristik citra yang berpotensi terdeteksi tidak benar?

1.3 Batasan Masalah

Karena luasnya ruang lingkup permasalahan dan pembahasan, maka tugas akhir ini diberikan batasan masalah sebagai berikut:

1. perangkat lunak yang digunakan adalah MATLAB,
2. *file* citra yang dapat dideteksi adalah *file* berformat .jpg dengan dimensi maksimal adalah 512x512 piksel yang terdiri dari layer luminance (grayscale) serta metode penyisipan citra tersebut menggunakan metode Jsteg yang merupakan *output* dari kode program MATLAB pada *file* jsteg.m.
3. panjang dan lebar citra yang tersisipi pesan habis dibagi dengan 8,
4. penyisipan pada citra stego menggunakan metode Jsteg dilakukan secara sekuensial,
5. pengambilan *file* stego dilakukan secara *offline*.

1.4 Tujuan Penelitian

Adapun tujuan yang hendak dicapai dari penyusunan tugas akhir ini, yaitu:

1. mengetahui ada atau tidaknya penyisipan pesan rahasia dalam citra digital dengan format jpg,
2. mengetahui daya analisis metode Uji *Chi-square* untuk mendeteksi sebuah *file* terstego dan tidak terstego dari persentase hasil pengujian,
3. dapat mengetahui perbedaan karakteristik citra yang berpotensi terdeteksi dengan baik dan terdeteksi tidak terlalu baik

1.5 Metodologi Penelitian

Metode penelitian yang akan digunakan dalam penyusunan tugas akhir ini terdiri dari:

1. Tahap Studi Kepustakaan

Melakukan studi kepustakaan terhadap berbagai referensi yang berkaitan dengan penelitian yang dilakukan. Studi kepustakaan ini bertujuan untuk mengumpulkan data-data yang dibutuhkan sebagai dasar teori untuk perancangan dan analisis yang akan dilakukan. Topik-topik yang akan dikaji antara lain meliputi: pengolahan citra digital, metode-motode steganografi, metode steganalisis menggunakan *Uji Chi-square Analysis* pada citra stego dengan metode penyisipan Jsteg pada citra jpg.

2. Tahap Pengumpulan Data

Pada tahap ini akan dilakukan pengumpulan *file-file* citra yang didalamnya terdapat pesan rahasia dengan cara steganografi dan *file-file* citra yang bersih (tidak ada pesan rahasia di dalamnya). Pengumpulan dilakukan dengan menggunakan program steganografi Jsteg yang telah dibuat sebelumnya.

Citra tidak tersisipi pesan merupakan citra bitmap yang disimpan ke dalam bentuk jpg dengan tidak menyisipkan pesan sama sekali. Sedangkan citra yang tersisipi pesan merupakan citra bitmap yang disimpan kedalam bentuk jpg dengan menyisipkan pesan pada domain DCTnya.

4. Tahap Perancangan dan Implementasi Sistem

Merancang sistem pendeteksian *file* citra yang dapat mengeluarkan output berupa ada atau tidaknya pesan tersembunyi pada *file* citra tersebut dengan melihatnya dari persentase terdeteksinya pesan sisipan dalam suatu citra. Jika persentase citra uji bernilai 50%, hal tersebut berarti dicurigai 50% dari citra uji sudah tersisipi pesan.

4. Tahap Analisis

Pada tahap ini, akan menganalisis dan menentukan seberapa besar tingkat keakuratan sistem dan seberapa besar ketahanan sistem terhadap noise yang ada di *file* citra, Juga berapakan waktu komputasi yang dibutuhkan untuk mendeteksi sebuah *file*.

5. Penyusunan Buku Tugas Akhir

Pada tahap ini disusun buku sebagai dokumentasi dari pelaksanaan Tugas Akhir, yang mencakup seluruh konsep, teori, implementasi, serta hasil analisis yang telah dikerjakan.

1.6 Sistematika Penulisan

BAB 1 Pendahuluan

Bab ini menjelaskan latar belakang masalah, rumusan masalah, batasan masalah, tujuan, manfaat, metodologi penelitian, dan sistematika penulisan tugas akhir.

BAB 2 Dasar Teori

Bab ini menjelaskan teori dasar yang mendukung dalam penyusunan perancangan sistem.

BAB 3 Perancangan Sistem

Bab ini menjelaskan bagaimana membangun sistem berdasarkan masalah yang diangkat, serta menyimulasikan sistem dengan asumsi yang ada.

BAB 4 Analisis Hasil Simulasi

Bab ini membahas analisis dari hasil perancangan sistem yang telah diaplikasikan.

BAB 5 Kesimpulan dan Saran

Bab ini berisi kesimpulan yang dapat ditarik dari hasil simulasi serta saran bagi para pembaca untuk dapat mengembangkan tugas akhir ini.

Telkom
University

BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

1. Metode *chi-square* dapat mendeteksi ada atau tidaknya pesan rahasia pada suatu data dengan melihat nilai frekuensi keluaran setiap koefisien atau piksel.
2. Akurasi maksimum untuk pendeteksian pada *background* statis terdapat pada skema 1 yaitu 89,109% dengan $\alpha=0.75$ dan 0.82 serta akurasi maksimum untuk citra *background* non statis adalah 91,794% pada skema 2 dengan $\alpha=0.88$.
3. Semakin kecil nilai alpha akan semakin tinggi nilai *p-value* karena banyak sample yang terdeteksi mengandung pesan stego.
4. Akurasi citra stego dan non stego terdeteksi benar tertinggi adalah pada saat menggunakan skema 1, yaitu mencapai 100% untuk citra stego dan 100% untuk citra non stego.
5. Pada citra dengan *background* statis yang memiliki selisih antar piksel yang berdekatan mendekati 0, akan selalu terdeteksi pesan. Karena nilai statis pada awal citra akan menghasilkan *p-value*=1.
6. Citra dengan *background* non-statis berpotensi lebih baik untuk akurasi deteksi yang lebih baik dibandingkan dengan citra dengan *background* statis, karena nilai *p-valuenya* yang stabil saat terjadi penurunan.
7. Proses menggunakan skema 1 menghasilkan *p-value* yang lebih linier namun membutuhkan waktu proses yang lama.
8. Proses menggunakan skema 2 menghasilkan persentase yang lebih stabil, namun dengan *p-value* yang kurang linier dan kurang stabil jika dibandingkan dengan skema 1. Waktu yang dibutuhkan untuk proses lebih cepat dari skema 1.

5.2 Saran

1. Steganalisis dilakukan untuk mendeteksi penyisipan yang bersifat *random*.
2. Dapat mendeteksi penyisipan yang tidak hanya dilakukan pada layer luminace saja, tapi dapat memanfaatkan semua layer.
3. Sistem dibuat pada bahasa perograman lain, seperti Java, C# dan bahasa pemrograman lainnya.

DAFTAR PUSTAKA

- [1] Bateman, Philip. *IMAGE STEGANOGRAPY AND STEGANALYSIS*. Retrieved April, 27, 2013. From website:
<http://www.computing.surrey.ac.uk/personal/st/H.Schaathun/projects/Past/p hil-msc.pdf>
- [2] Junaedi, Danang dkk. *STEGANOGRAPHY & WATERMARKING*. Retrieved Mei 12, 2013. From website:
<https://danangjunaedi.files.wordpress.com/2011/02/citra-sesi12-steganografi-watermarking.pdf>
- [3] Kurniawan, Yosep. *STUDI METODE STEGANALISIS PADA STEGOIMAGE*. Retrieved Mei 20, 2013. From website:
<http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2006-2007/Makalah1/Makalah1-031.pdf>
- [4] Li, Bin dkk. (2010, Oktober). *A Survey on Image Steganography and Steganalysis*. Retrieved April 24, 2013. From website:
<http://bit.kuas.edu.tw/~jihmsp/2011/vol2/JIH-MSP-2011-03-005.pdf>
- [5] Prabowo, Praditya Harry dkk. *ANALISIS DAN PERANCANGAN STEGANOGRAFI PADA FILE JPEG DENGAN MENGGUNAKAN ALGORITMA F5*. Retrieved January 15, 2014. From website:
<http://thesis.binus.ac.id/doc/Bab2/LBM2006-361-Bab%202.pdf>
- [6] Pradito, Pandu. *JPEG*. Retrieved Mei 13, 2013. From website:
<http://blog.ub.ac.id/yafemo/files/2011/07/JPEG.doc>
- [7] Susanto, Arnold Nugroho. *STUDI ANALISIS TEKNIK-TEKNIK PENDETEKSIAN STEGANOGRAFI DENGAN METODE LSB DALAM MEDIA GAMBAR*. Retrieved Mei 20, 2013. From website:
http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2009-2010/Makalah1/Makalah1_IF3058_2010_005.pdf
- [8] Tim IMV. 2010. *Image Processing and Vision*. Institut Teknologi Telkom: Bandung.

- [9] Fridrich, Jesica dan Miroslav Goljan. *Practical Steganalysis of Digital Images – State of the Art*. Retrieved: April 27, 2013. From website: <http://ws2.binghamton.edu/fridrich/Research/steganalysis01.pdf>
- [10] Toumazis, Alex. 2009. *Steganography*. Retrieved: januari 10, 2014. From website: <http://www.cl.cam.ac.uk/teaching/0910/R08/work/essay-at443-steganography.pdf>

